Analysis of the PROFIBUS Token Passing Protocol over Wireless Links

Andreas WILLIG, Member, IEEE
Telecommunication Networks Group, Technical University Berlin
email: awillig@ieee.org

***Abstract*— For the PROFIBUS, a standardized and well-known fieldbus system, it is attractive to use wireless media. A natural approach in creating such a system is to re-use as much existing technology as possible. In the area of wireless local area networks (WLANs) clearly the IEEE 802.11 standard is the leading technology. Hence, the question comes up, how this technology can be used in the creation of a wireless PROFIBUS. In this paper we consider the solution of running the existing PROFIBUS MAC and link-layer protocol directly on top of an IEEE 802.11 DSSS PHY, without the 802.11 MAC functionality. We show that the PROFIBUS MAC protocol (a token-passing scheme on top of a broadcast medium, stations organized in a logical ring) is vulnerable against bit errors and packet losses. Specifically, the membership of a station in the logical ring is harmed by loss of token frames. Ring membership is important, since only ring members are allowed to transmit data. Lost stations can't do so, no matter how time-critical and important their data is. Their re-inclusion into the ring takes some time. The problems are serious and we conclude that for creation of a wireless PROFIBUS alternative solutions for MAC- and link-layer protocols should be investigated.**

I. Introduction

The topic of a wireless fieldbus in general, and a wireless PROFIBUS in particular is up in the air, due to several benefits of wireless technologies, including mobility and reduced cabling need. A natural approach in creating such a system is to re-use as much existing technology as possible. In the area of wireless local area networks (WLANs) clearly the IEEE 802.11 standard is the leading technology [5], [7], [6]. Hence, the question comes up, how this technology can be used in the creation of a wireless PROFIBUS.

In this paper we consider the solution of just taking the physical layer of IEEE 802.11 (namely, the mostly-deployed direct sequence spread spectrum (DSSS) PHY) and to run the PROFIBUS medium access control (MAC) and link-layer protocol directly on top of this PHY, leaving out the 802.11 MAC. The hope is that the desirable properties of the PROFIBUS protocol, namely its realtime behavior, carries over to the wireless case.

In this paper we show that this hope does not take far. We investigate the behavior of the PROFIBUS MAC protocol when operated over a wireless-type link. This type of link brings not only the phenomena of bit errors and packet losses, but also some of the PROFIBUS protocol features will not work, due to the disability to send and receive simultaneously from the wireless medium. The PROFIBUS MAC protocol employs a token-passing scheme on top of a broadcast medium. The protocol passes the token along the members of a logical ring. The right to initiate transmissions is tied to own the token. This has the consequence that only ring members will obtain the right to transmit data from time to time.

The results presented in this paper show that the PROFIBUS protocol has serious problems with the stability of the logical ring when operated over a wireless type link. PROFIBUS stations get lost from the ring due to repeated losses of token frames caused bit errors and packet losses, and it takes some time to re-include them. During this time they have no possibility to transmit data, which in turn affects their ability to deliver high priority messages within time.

An investigation of the PROFIBUS protocol on top of a wired medium and taking only bit errors into account is presented in [10] and [15]. The difference between the present study and the results presented there seems small, but it significant: in the wired medium case a station can read back the signals from the medium (*hearback*) and can check for differences, on a wireless medium this does not work. In the cited papers the so-called *ring-jacking* scenario was identified as dominant source of ring instability. In this scenario the ring was destroyed under specific circumstances in one step by a single station. However, this scenario relies critically on a working hearback feature, which cannot be assumed in wireless media.

This paper is structured as follows: in the next Section II we give the necessary background information on the PROFIBUS and the error behavior of an IEEE 802.11 wireless link. In Section III we discuss the results and the setup of a simulation study carried out to assess the ring stability of the PROFIBUS protocol over wireless links. Finally, after reviewing related work in Section IV we give the conclusions in Section V.

II. Background

This section summarizes briefly the PROFIBUS protocol, the main features of the IEEE 802.11 DSSS PHY and the wireless channel models.

A. PROFIBUS

The PROFIBUS fieldbus ([2], with some corrections in [8]) is standardized and widely used in Europe. It exists in several versions, called “profiles”. The FMS version (Fieldbus Message Specification) is defined on layers 1, 2, and 7 of the OSI reference model. On the PHY often RS 485 is employed, the MAC layer implements a token passing protocol on top of a broadcast medium. Stations participating in the token-passing process are called active stations.

An active station is only allowed to transmit data, if it owns the token. The token holding time is bounded by a variant of the timed-token protocol (with target token rotation time T_{TTRT}), and after it expires, the token-owner is required to pass the token to the next active station. The active stations form a logical ring. They are responsible for ring maintenance, namely, for including new stations into the ring (they do so by regularly polling the address range between themselves and their logical successor). Passing the token from station a to station b involves transmitting a token frame. After a has sent this frame, it listens for a short time (called slot time, T_{SL} on the medium, whether there is some activity (a infers from this that b has accepted the token). If there is no activity, the token frame is retransmitted. After three unsuccessful trials, a determines b's logical successor in the ring (say, c) and tries to pass the token to c, and b is lost from the ring. It is a's responsibility to re-include b later on, but this may take some time (depending on certain protocol parameters and the current load).

New stations are included by stations already present in the ring: a ring member polls approximately every *gap_factor* $\cdot$ T_{TTRT} seconds the address space between its own address and that of its logical ring successor. If a new station is found, it is included into the ring.

B. IEEE 802.11 and Wireless Link Models

A wireless link in the 2.4 GHz ISM band differs from cable-based links: it is much more error-prone and it has time-variable behavior. It can happen that a link is rather good for then minutes, and absolutely unusable for the next three minutes. Errors on wireless links occur due to different phenomena, namely multipath fading, path loss, co- and adjacent channel interference, man-made interference (microwave ovens, remote controls) and simple noise.

An important finding discussed in reference [14] is that errors occur not only due to simple bit errors (where single or multiple bits in a packets data part change their value), but also due to packet losses. In the latter case the wireless receiver fails to acquire bit synchronization during a packet's preamble. For the receiver a lost packet is not distinguishable from a packet not sent at all. In reference [14] it is shown that packet losses tend to occur in bursts. While these are mostly smaller than ten packets, occasionally very long bursts of lost packets were observed.

For evaluating the behavior of MAC- and link-layer protocols over wireless links one typically resorts to stochastic models. These kinds of models employ a (typically simple) stochastic process, which in turn depends on some parameters. A very popular model is the "Gilbert-Elliot" error model [9], [3], [1]. However, in this paper we restrict to the simple case of independent bit errors and independent packet losses.

III. Results

We show the results made with a PROFIBUS simulator already described in [10] and [15]. The simulator implements parts of the PROFIBUS link layer, the PROFIBUS MAC protocol and a shared medium. For this study the shared medium is wireless-type with the following characteristics:

- The medium can show packet losses in addition to bit errors.
- No station can read back its own transmissions from the medium. This avoids the "ring-jacking" and "hearback-removal" scenarios described in [15], but also removes the ability to detect collisions.
- PROFIBUS frames are embedded into 802.11 PHY packets. A PHY packet consists of an 128 μs preamble (for acquiring bit synchronization) and some PHY header fields (e.g., indicating the overall length of the packet and the modulation type of the packets data part), taking another 64 μs. However, in contrast to the RS-485 version of PROFIBUS every byte is transmitted with eight bits instead of eleven.
- Every frame, including token frames, is equipped with a 16 bit CRC checksum, which is assumed to work perfectly.

Two simple sets of simulations were performed, differing in their respective bit error rate (BER): the first set uses independent bit errors with a BER of 10^{-3}, in the second set there occur no bit errors. In both sets there occur packet losses with a certain packet loss rate (PLR), which is varied from 0.0 to 0.1 in steps of 0.01, assuming independent packet losses. These PLR's are well in the range observed by measurements [14] and are not amongst the worst observed PLR's.

The scenario consists of $K = 10$ stations with no data load, in order to highlight the issues related to ring stability. The fixed simulation parameters are summarized in Table I. The simulations are run for 3600 simulated seconds.

The main ring stability measures investigated are:

- the mean number of stations in the ring $\bar{N}(t)$ taken over the simulation time t, and
- the fraction of time $\bar{M}(t)$ that the ring has not the full number of members taken over simulation time t (clearly, $\bar{M}(t) = 0$ is the best achievable value, $\bar{M} = 1$ the worst one).

For the case without bit errors in Figure 1 the $\bar{N}(3600)$ values are presented for varying PLR, while in Figure 2 the $\bar{M}(3600)$ values are displayed. Respectively, for the case with bit errors the corresponding Figures are Figure 3 for the $\bar{N}(3600)$ values and 4 for the $\bar{M}(3600)$ values. The following points are important:

- The ring stability is sensitive to packet losses. Even for 6% packet losses without bit errors $\approx$ 50% of the time the ring is not full. Enabling two protocol improvements presented in [15], namely a new timeout timer calculation method, and a method for fast re-inclusion of lost stations, we can reduce this fraction to $\approx$ 30%. However, both is hardly acceptable for time critical communications. If in addition bit errors occur, with both improvements enabled the ring is not full for $\approx$ 56% of the time, while the unchanged protocol completely breaks down and is for $\approx$ 78% of the time not complete.
- In all figures the curves for the unmodified protocol and

Parameter	Value
# of stations	$K = 10$
gap factor	$g = 6$
target token rotation time	$T_{TTRT} = 20$ msec
bit rate	$b = 1$ MBit/s
protocol slot time	T_{SL} = 400 μs
station delay	100 μs

TABLE I

FIXED PARAMETERS FOR RING STABILITY SIMULATIONS OVER WIRELESS CHANNEL

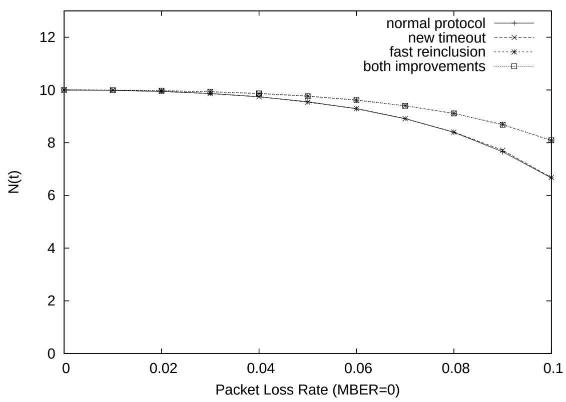

Fig. 1. $\bar{N}(3600)$ vs. PLR (independent packet losses) and no bit errors

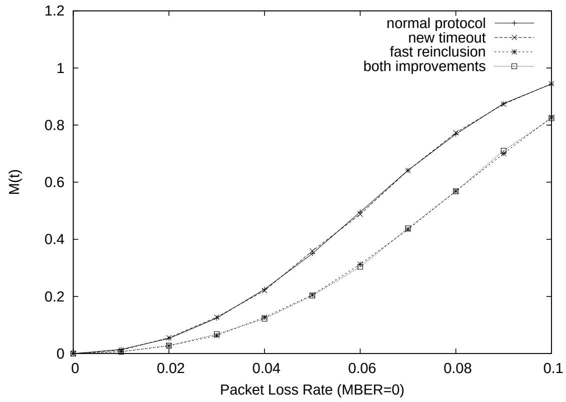

Fig. 2. $\bar{M}(3600)$ vs. PLR (independent packet losses) and no bit errors

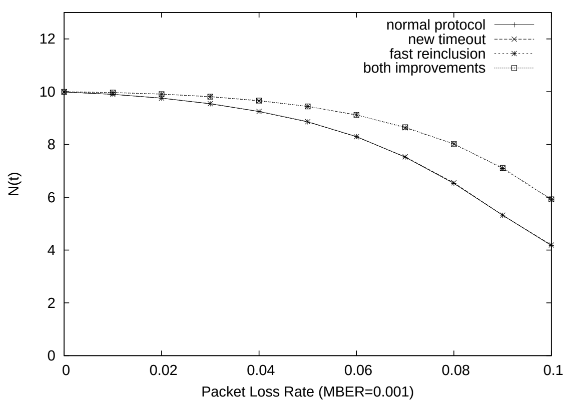

Fig. 3. $\bar{N}(3600)$ vs. PLR (independent packet losses) and BER of 10^{-3}

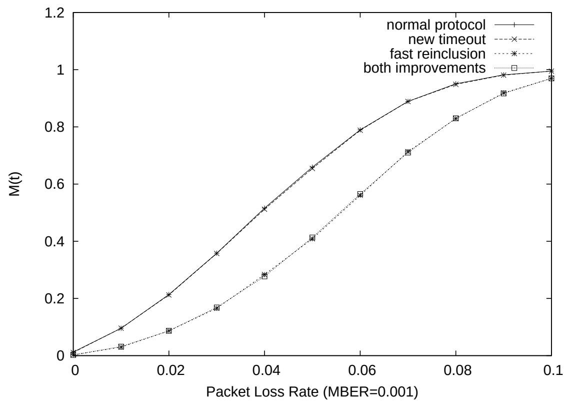

Fig. 4. $\bar{M}(3600)$ vs. PLR (independent packet losses) and BER of 10^{-3}

the protocol with the new timeout computation method lie very close together, the same holds for the curves for both improvements and the fast reinclusion feature. Hence, only the fast reinclusion feature gives some gain in ring stability, while the timeout method gains nothing. For the case with a wired-medium the opposite behavior could be observed [15]. This can be explained by the fact that the timeout method is useful in preventing the ring-jacking scenario, which relies on the hearback feature not available in wireless media.

A careful inspection of the results and the simulators logfiles indicate that the major source of ring instability is simply that token frames do not reach their destination, which in turn get lost from the ring. Since this is required to lose three consecutive token frames, the independent bit error / packet loss model is in favor or the PROFIBUS protocol, since even with a packet loss rate of 10% the station loss probability is 0.001. This is different in bursty error models, even with the same mean packet loss rate: within an packet loss burst the packet loss rate is much higher than for the case of independent packet losses, since it has to compensate for the packet loss free bursts. Hence, when the channel is in a bad state, it is more likely to lose three consecutive token packets.

To provide evidence on the difference between channel error models, we show some results on another set of simulations, which are carried out with the same PROFIBUS simulator, however, with some important differences [11], [12]:

- We have chosen four different error models, three of them (*independent*, *Gilbert-Elliot*, *Semi-Markov*) parameterized from a specific trace (trace 24) of the measure-

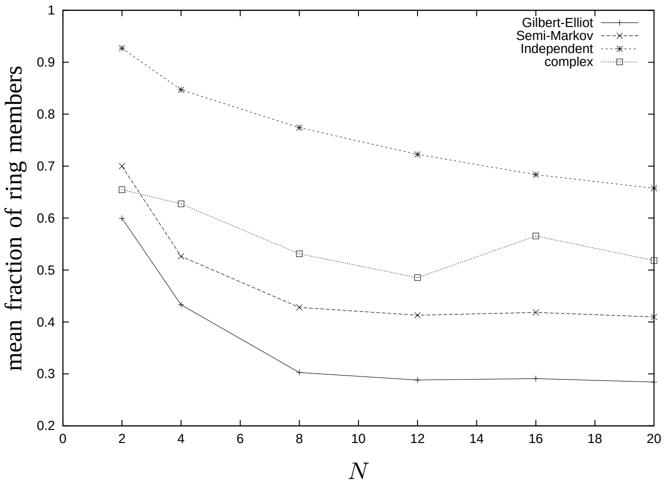

Fig. 5. Fraction of the mean number of PROFIBUS ring members to the overall number of stations vs. number of stations for the PROFIBUS protocol, all error models and 50% low priority load

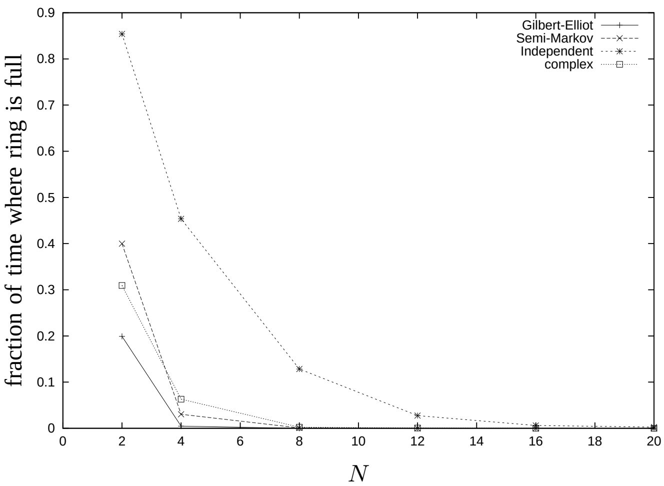

Fig. 6. Fraction of time that the PROFIBUS logical ring is complete vs. number of stations N for all error models and 50% low priority load

ments reported in [14] (with a BER of 0.00037 and a PLR of $\approx$ 0.11), and the fourth (*complex*) parameterized from four different traces. The bit errors and packet losses exhibited by trace 24 are very variable. While the independent model captures only the mean bit error / packet loss rate, the Gilbert-Elliot captures the mean bit error / packet loss burst lengths (bit-error free / packet loss free burst lengths) of the trace, while the Semi-Markov model additionally captures the variances. The complex model is of increased statistical accuracy.

- For every pair of PROFIBUS stations there is a separate channel error model independent of the other ones.
- The number of stations was varied from $N = 2$ up to $N = 20$, and the system was loaded with low priority data.
- The simulations are carried out for several values of T_{TTRT} and gap factor, chosen such that re-inclusion happens very fast.

In Figure 5 we show the mean fraction of ring members vs. the number of stations N in the logical ring, and in Figure 6 we show the fraction of time that the ring is complete vs. number of stations N. The latter is actually one minus $\bar{M}(3600)$. Please note that we show the best values achieved over all simulated T_{TTRT} and gap factor values. The following points are remarkable:

- For the bursty error models (Gilbert-Elliot, Semi-Markov and complex) the mean number of members in the ring is almost below 60% (Fig. 5), and reaches values below 30% for the Gilbert-Elliot model. Things look better for the independent model. The same relationship between the error models can be seen for the fraction of times that the ring is full.
- There is a dependency on the number of stations N, such that for increasing N the ring becomes less stable. This can be explained as follows: since the T_{TTRT} values were limited, with a higher number of stations due to the protocol operation a larger number of token passing trials per second take place, which translates into more opportunities to lose stations from the ring.

IV. Related Work

Some references on related work regarding wireless fieldbus systems and wireless PROFIBUS systems can be found in [13], which contains a proposal for an alternative MAC protocol for a wireless PROFIBUS. Other proposals can be found in [11], [12]. All these proposes use a polling-based approach, introducing a base station (BS) and one-time registration of a station with the BS. Hence, the concept of a logical ring and ring-membership is eliminated.

The issue of the vulnerability of the logical token-passing ring for the case of the IEEE 802.4 Token-Bus protocol is investigated in [4] using analytical techniques and measurements. It is shown, how bursty errors affect the token passing process, and how this in turn affects the mean token passing time and, more important, the mean token rotation time.

V. Conclusions

To summarize, the original PROFIBUS protocol behaves inacceptable for moderate packet loss rates of 5% to 10%, as observed in measurements. This is true for both the unmodified protocol as well as for an enhanced version of the protocol. The improvements do not avoid packet losses, only the fast re-inclusion method helps to re-construct the ring somewhat faster. Our analysis has shown that the concept of permanently relying on token frames for the purpose of ring maintenance is vulnerable to channel errors. Specifically the loss of whole frames (token frames) affects the stability.

The bad thing about ring instability is that it may take some time to re-include lost members. During these outage times the stations are not allowed to transmit data, no matter how time-critical or urgent they are.

Another disadvantage of explicit token passing not discussed so far is the fact that it explicitly requires a fully meshed topology, i.e., every station must be able to hear all other stations. Modifying the token passing process such that partially meshed topologies are possible and can be integrated with a wired PROFIBUS segment is at least challenging.

These results lead us to believe, that for this type of error-prone and time-variable links, it is worthwhile to investigate different types of MAC protocols for a wireless PROFIBUS.

REFERENCES

[1] E. O. Elliot. Estimates of error rates for codes on burst-noise channels. *Bell Systems Technical Journal*, 42:1977–1997, September 1963.

[2] German Institute of Standardization (DIN). *PROFIBUS Standard Part 1 and 2*, 1991.

[3] E. N. Gilbert. Capacity of a burst-noise channel. *Bell Systems Technical Journal*, 39:1253–1265, September 1960.

[4] Hong ju Moon, Hong Seong Park, Sang Chul Ahn, and Wook Hyun Kwon. Performance Degradation of the IEEE 802.4 Token Bus Network in a Noisy Environment. *Computer Communications*, 21:547–557, 1998.

[5] The Editors of IEEE 802.11. *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, November 1997.

[6] The Editors of IEEE 802.11. *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher speed Physical Layer (PHY) extension in the 2.4 Ghz band*, 1999.

[7] The Editors of IEEE 802.11. *IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band*, 1999.

[8] PROFIBUS Nutzerorganisation e.V., PROFIBUS Nutzerorganisation e.V., Haid-und-Neu-Str. 7, Karlsruhe, Germany. *Implementation Guide to DIN 19245 Part 1*, August 1994.

[9] H.S. Wang and N. Moayeri. Finite State Markov Channel - A Useful Model for Radio Communication Channels. *IEEE Transactions on Vehicular Technology*, 44(1):163–171, February 1995.

[10] Andreas Willig. Analysis of the PROFIBUS Token Passing Protocol over Error Prone Links. In *Proc. 25th Annual Conference of the IEEE Industrial Electronics Society (IECON'99)*, pages 1246 – 1252. IEEE, November 1999.

[11] Andreas Willig. Polling-based MAC Protocols for Improving Realtime Performance in a Wireless PROFIBUS. *IEEE Transactions on Industrial Electronics*, 2002. submitted.

[12] Andreas Willig. Polling-based MAC Protocols for Improving Realtime Performance in a Wireless PROFIBUS – Extended Version. TKN Technical Report Series TKN-02-003, Telecommunication Networks Group, Technical University Berlin, April 2002.

[13] Andreas Willig. The Adaptive-Intervals MAC protocol for a wireless PROFIBUS. In *Proc. 2002 IEEE International Symposium on Industrial Electronics*, 2002. accepted.

[14] Andreas Willig, Martin Kubisch, Christian Hoene, and Adam Wolisz. Measurements of a Wireless Link in an Industrial Environment using an IEEE 802.11-Compliant Physical Layer. *IEEE Transactions on Industrial Electronics*, 2001. accepted for publication.

[15] Andreas Willig and Adam Wolisz. Ring Stability of the PROFIBUS Token Passing Protocol over Error Prone Links. *IEEE Transactions on Industrial Electronics*, 48(5):1025–1033, October 2001.